

**In the Claims**

Claims 1, 5, 11-13, 16, 27, 36, 37, 41 and 42 are amended.

Claims 4, 14, 17, 18 and 34 are canceled.

Claims 1-3, 5-13, 15, 16, 19-33 and 35-42 remain in the application and are listed just below:

1. (Currently Amended) A method of updating keys that decrypt login tickets that log a user into multiple sites, the method comprising:

generating a first key having a first version number;

providing tickets encoded consistent with the first key, the ticket having a version number corresponding to the first version number,

generating a second key having a second version number; and when the second key becomes current at a site, providing tickets encoded consistent with the second key, the ticket having a version number corresponding to the second version number;

~~wherein said tickets are configured to enable a user to access and use one or more affiliated servers without requiring any additional authentication information other than authentication information originally provided by the user to an authentication server~~ said keys comprise key data and executable code for decrypting tickets.

2. (Original) The method of claim 1 wherein a different key is provided to each site, and wherein each key is encrypted for decoding at one site.

1           3.     (Original) The method of claim 1 and further including generating a  
2 configuration file to track keys for each site.

3  
4           4.     (Canceled).

5  
6           5.     (Currently Amended) A computer readable medium having  
7 instructions stored thereon for causing a computer to perform a method of updating  
8 keys that decrypt login tickets that log a user into multiple sites, the method  
9 comprising:

10           generating a first key having a first version number;

11           providing tickets encoded consistent with the first key, the ticket having a  
12 version number corresponding to the first version number;

13           generating a second key having a second version number; and

14           when the second key becomes current at a site, providing tickets encoded  
15 consistent with the second key, the ticket having a version number corresponding to  
16 the second version number;

17           ~~wherein said tickets are configured to enable a user to access and use one or~~  
18 ~~more affiliated servers without requiring any additional authentication information~~  
19 ~~other than authentication information originally provided by the user to an~~  
20 ~~authentication server~~ said keys comprise key data and executable code for decrypting  
21 tickets.

22  
23           6.     (Original) A method of generating keys that decrypt login tickets that  
24 log a user into multiple sites, the method comprising:

25

1 generating a first key in the form of an executable having a first version  
2 number;

3 generating a second key in the form of an executable having a second version  
4 number; and

5 providing an indication to a login server identifying which key is current for  
6 each site such that the tickets are properly encoded.

7  
8 7. (Original) The method of claim 6 and further comprising distributing  
9 the key to multiple login servers in a secure manner.

10  
11 8. (Original) The method of claim 6 and further comprising updating a  
12 configuration file to track keys for each site.

13  
14 9. (Original) A computer readable medium having instructions stored  
15 thereon for causing a computer to perform a method of generating keys that decrypt  
16 login tickets that log a user into multiple sites, the method comprising:

17 generating a first key in the form of an executable having a first version  
18 number;

19 generating a second key in the form of an executable having a second version  
20 number; and

21 providing an indication to a login server identifying which key is current for  
22 each site such that the tickets are properly encoded.

23  
24 10. (Original) A system that generates keys that decrypt login tickets that  
25 log a user into multiple sites, the system comprising:

1 a key generator that generates a first key in the form of an executable having a  
2 first version number and generates a second key in the form of an executable having  
3 a second version number; and

4 means for providing information to a login server identifying which key is  
5 current for each site such that the tickets are properly encoded.

6  
7 11. (Currently Amended) A method of updating keys that decrypt login  
8 tickets that log a user into multiple sites, the method comprising:

9 generating a new key with an incremented version number;

10 sending the new key to a partner site for use in decoding tickets with the  
11 incremented version number;

12 updating key and version information for a login server; and

13 generating tickets decodable by the new key when an indication that a key  
14 having a previous version number has expired;

15 wherein said tickets are configured to enable a user to access and use one or  
16 more affiliated servers without requiring any additional authentication information  
17 other than authentication information originally provided by the user to an  
18 authentication server said keys comprise key data and executable code for decrypting  
19 tickets.

20  
21 12. (Currently Amended) A computer readable medium having  
22 instructions stored thereon for causing a computer to perform a method of updating  
23 keys that decrypt login tickets that log a user into multiple sites, the method  
24 comprising:

25 generating a new key with an incremented version number;

1 sending the new key to a partner site for use in decoding tickets with the  
2 incremented version number;

3 updating key and version information for a login server; and

4 generating tickets decodable by the new key when an indication that a key  
5 having a previous version number has expired;

6 wherein ~~said tickets are configured to enable a user to access and use one or~~  
7 ~~more affiliated servers without requiring any additional authentication information~~  
8 ~~other than authentication information originally provided by the user to an~~  
9 ~~authentication server~~ said keys comprise key data and executable code for decrypting  
10 tickets.

11  
12 13. (Currently Amended) A method of updating a key used to decrypt  
13 tickets used to log into a site, the method comprising:

14 receiving an updated key with a new version number;

15 setting a time for an old current key having an old version number to expire;

16 making the updated key the current key;

17 wherein ~~said tickets are configured to enable a user to access and use one or~~  
18 ~~more affiliated servers without requiring any additional authentication information~~  
19 ~~other than authentication information originally provided by the user to an~~  
20 ~~authentication server~~ at least one of said keys comprise executable code for making  
21 the updated key the current key.

22  
23 14. (Cancel).  
24  
25

1           15. (Original) The method of claim 13 and further comprising redirecting  
2 users attempting to log into the site using the old current key.

3  
4           16. (Currently Amended) A computer readable medium having  
5 instructions stored thereon for causing a computer to perform a method of updating a  
6 key used to decrypt tickets used to log into a site, the method comprising:

7           receiving an updated key with a new version number;

8           setting a time for an old current key having an old version number to expire;

9           making the updated key the current key;

10          ~~wherein said tickets are configured to enable a user to access and use one or~~  
11 ~~more affiliated servers without requiring any additional authentication information~~  
12 ~~other than authentication information originally provided by the user to an~~  
13 ~~authentication server~~ wherein at least one of said keys comprise executable code for  
14 making the updated key the current key.

15  
16          17. (Canceled).

17  
18          18. (Canceled).

19  
20          19. (Original) A method of managing keys used to decrypt tickets for  
21 logging onto a site, the method comprising:

22          receiving a first key with a first version number;

23          encrypting the first key using a hardware address;

24          changing a current key variable to the first version number;

25          receiving a new key with an incremented version number;

1 encrypting the new key using a hardware address; and  
2 identifying the new key as the current key.

3  
4 20. (Previously Presented) The method of claim 19 and further comprising  
5 setting a time for the first key identifying when such key may no longer be used.

6  
7 21. (Original) The method of claim 20 wherein a user currently logged in  
8 may continue to use the first key until the time expires.

9  
10 22. (Original) The method of claim 20 wherein new user may only use a  
11 ticket corresponding to the second key when the second key is made the current key.

12  
13 23. (Original) The method of claim 20 wherein the time is set to a  
14 reauthorization time determined by the site.

15  
16 24. (Original) The method of claim 19 wherein a new user using a  
17 previous version ticket will be redirected to obtain a ticket corresponding to the new  
18 key following the new key being identified as the current key.

19  
20 25. (Original) The method of claim 19 wherein the new key is identified as  
21 the current key by changing the current key variable to the second version number.

22  
23 26. (Original) A computer readable medium having instructions stored  
24 thereon for causing a computer to perform a method of managing keys used to  
25 decrypt tickets for logging onto a site, the method comprising:

1 receiving a first key with a first version number;  
 2 encrypting the first key using a hardware address;  
 3 changing a current key variable to the first version number;  
 4 receiving a new key with an incremented version number;  
 5 encrypting the new key using a hardware address; and  
 6 identifying the new key as the current key.

7  
 8 27. (Currently Amended) A method of updating keys used to decrypt  
 9 tickets used to log into multiple sites on a network, the method comprising:

10 generating a new key with a new version number to take the place of an old  
 11 key with an old version number;

12 storing the new key on a site to be logged into by a user;

13 changing a current key indication to the new key;

14 allowing current logged in users to continue using the old key; and

15 redirecting new users to a login server to obtain a ticket consistent with the  
 16 new key;

17 wherein keys are generated in an executable form which includes key  
 18 information as well as code for decrypting tickets using the key information.

19  
 20 28. (Original) The method of claim 27 wherein the old key may be used  
 21 by current logged in users for a predetermined amount of time.

22  
 23 29. (Original) The method of claim 28 wherein the predetermined amount  
 24 of time is no more than a reauthorization time by which a current user is normally  
 25 required to provide login information.



1  
2 30. (Original) The method of claim 28 wherein the predetermined amount  
3 of time may be set to zero to force all current and new users to login with a ticket  
4 consistent with the new key version.

5  
6 31. (Original) The method of claim 27 wherein the ticket contains a  
7 version number consistent with the version number of the key which can decrypt it.

8  
9 32. (Original) The method of claim 27 wherein keys are encrypted by the  
10 site using a hardware address, and stored by the site.

11  
12 33. (Original) The method of claim 27 wherein a new key is generated  
13 based on a request of the site.

14  
15 34. (Canceled).

16  
17 35. (Original) The method of claim 27 wherein the keys are generated by  
18 an authentication server, mad are distributed to multiple login servers for providing  
19 login tickets.

20  
21 36. (Currently Amended) A computer readable medium having  
22 instructions stored thereon for causing a computer to perform a method of updating  
23 keys used to decrypt tickets used to log into multiple sites on a network, the method  
24 comprising:  
25

1 generating a new key with a new version number to take the place of an old  
2 key with an old version number;  
3 storing the new key on a site to be logged into by a user;  
4 changing a current key indication to the new key;  
5 allowing current logged in users to continue using the old key; and  
6 redirecting new users to a login server to obtain a ticket consistent with the  
7 new key,  
8 wherein the keys comprise key data and executable code for decrypting  
9 tickets.

10  
11 37. (Currently Amended) A method of logging on to multiple sites, the  
12 method comprising:

13 sending a first login ticket to a desired site, wherein the login ticket is  
14 encrypted to be decoded by a first key having a first version number;

15 receiving an indication that the first key has expired;

16 obtaining a second login ticket from an authentication server, wherein the  
17 second login ticket is encrypted consistently with a new key having a second version  
18 number; and

19 sending the second login ticket to the site to log into the site;

20 ~~wherein said tickets are configured to enable a user to access and use one or~~  
21 ~~more affiliated servers without requiring any additional authentication information~~  
22 ~~other than authentication information originally provided by the user to an~~  
23 ~~authentication server~~ the keys comprise key data and executable code for decrypting  
24 tickets.

1        38. (Original) The method of claim 37 wherein the tickets contain a  
2 version number which is readable without decryption.

3  
4        39. (Original) The method of claim 38 wherein the version number is a  
5 one digit Hex 5 integer.

6  
7        40. (Original) The method of claim 38 wherein the encrypted ticket  
8 comprises an unencrypted version number, and encrypted information sufficient to  
9 log a user into a desired site.

10  
11       41. (Currently Amended) A computer readable medium having  
12 instructions stored thereon for causing a computer to perform a method of logging on  
13 to multiple sites, the method comprising:

14       sending a first login ticket to a desired site, wherein the login ticket is  
15 encrypted to be decoded by a first key having a first version number;

16       receiving an indication that the first key has expired;

17       obtaining a second login ticket from an authentication server, wherein the  
18 second login ticket is encrypted consistently with a new key having a second version  
19 number; and

20       sending the second login ticket to the site to log into the site;

21       ~~wherein said tickets are configured to enable a user to access and use one or~~  
22 ~~more affiliated servers without requiring any additional authentication information~~  
23 ~~other than authentication information originally provided by the user to an~~  
24 ~~authentication server~~ the keys comprise key data and executable code for decrypting  
25 tickets.

1  
2 42. (Currently Amended) An encrypted ticket for use in logging on to a  
3 website, the ticket comprising:

4 an unencrypted version number corresponding to a key version number stored  
5 on the website; and

6 an encrypted string identifying the website and information, which when  
7 decrypted using the key having the same version number authenticates the user for  
8 logging the user into the website;

9 wherein said ticket is configured to enable a user to access and use one or  
10 more affiliated servers without requiring any additional authentication information  
11 other than authentication information originally provided by the user to an  
12 authentication server the key comprises executable code for decrypting tickets.